



Supplemental Notice of Data Event

March 14th, 2023

Independent Living Systems, LLC (“ILS”), which is a business associate to its covered entity subsidiaries Florida Community Care LLC and HPMP of Florida Inc. d/b/a Florida Complete Care, is issuing supplemental notice of a data event that may impact the privacy of certain individuals’ personal and/or protected health information (“PHI”). ILS is also issuing notification to impacted individuals as a direct provider of services and on behalf of certain data owner clients and covered entity health plans. We are providing updated information about the event and our response. We are unaware of any identity theft or fraud resulting from this event. We are providing this supplemental notice out of an abundance of caution.

What Happened?

On July 5, 2022, we experienced an incident involving the inaccessibility of certain computer systems on our network. We responded to the incident immediately and began an investigation with the assistance of outside cybersecurity specialists. Through our response efforts, we learned that an unauthorized actor obtained access to certain ILS systems between June 30 and July 5, 2022. During that period, some information stored on the ILS network was acquired by the unauthorized actor, and other information was accessible and potentially viewed. Upon containing the incident and reconnecting our computer systems, we conducted a comprehensive review to understand the scope of potentially affected information and identify the individuals to whom such information relates. We received the results of this review on January 17, 2023, and then worked as quickly as possible to validate the results and provide notice to potentially impacted individuals and affiliated data owners, as required under applicable law and contract.

What Information was Affected?

The types of impacted information varies by individual and could have included: name, address, date of birth, driver's license, state identification, Social Security number, financial account information, medical record number, Medicare or Medicaid identification, CIN#, mental or physical treatment/condition information, food delivery information, diagnosis code or diagnosis information, admission/discharge date, prescription information, billing/claims information, patient name, and health insurance information.

What We Are Doing.

We take this incident and the security of information entrusted to us very seriously. In response to the incident, we promptly took steps to mitigate any risk of compromise to information and better prevent a similar event from reoccurring. These actions included: (1) fortifying the security of our firewall; (2) utilizing the forensic specialists engaged to monitor our network and remediate any suspicious activity identified; (3) rotating and increasing the complexity of all users' credentials, and (4) providing notification to potentially affected individuals as quickly as possible. We are also enhancing our existing training protocols and other internal procedures that relate to data protection and security. In accordance with best practices, we encourage you to review your account statements, explanations of benefits, and credit reports carefully for unexpected activity and to report any questionable activity to the associated institutions immediately.

Additionally, we previously notified potentially affected individuals on September 2, 2022 by posting a preliminary notice of this data event on our website. We also provided preliminary notice to our primary state and federal regulators. Now that our review and validation efforts are complete, we are notifying potentially affected individuals via posting this supplemental notice on our website, providing notice to the media, and mailing letters to potentially affected individuals for whom ILS has address information. ILS is also providing supplemental notice to its primary state and federal regulators, initial notice to certain additional state regulators (as required), and initial notice to the three major consumer reporting agencies (i.e., Equifax, Experian, and TransUnion).

What Affected Individuals Can Do.

We encourage potentially affected individuals to remain vigilant against incidents of identity theft and fraud by reviewing their account statements, explanations of benefits, and credit reports carefully for unexpected activity and to report any questionable activity to the associated institutions immediately. Additional information can be found below in the Steps You Can Take to Protect Information.

For More Information.

For individuals seeking additional information regarding this event, a toll-free assistance line has been established. Individuals may call 800-906-7238 toll-free Monday through Friday from 8 am – 10 pm Central, or Saturday and Sunday from 10 am – 7 pm Central (excluding major U.S. holidays). Be prepared to provide your engagement number B086938. You may also write to ILS at P.O. Box 667955, Miami, FL 33166.

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Monitor Your Account

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert display on a consumer’s credit file, a business is required to take steps to verify the consumer’s identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer’s express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a credit freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;

3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax

<https://www.equifax.com/personal/credit-report-services/>

888-298-0045

Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069

Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788

Experian

<https://www.experian.com/help/>

1-888-397-3742

Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013

Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013

TransUnion

<https://www.transunion.com/credit-help>

TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016

TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-

4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further

information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; and oag@dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_yourrights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov/>.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are 64 Rhode Island residents impacted by this incident.

Contact Us

Learn more about how Independent Living Systems is enhancing individuals' quality of life by improving health outcomes, reducing costs, and addressing social risks.

305-262-1292

ABOUT US

[History](#)

[Executive Team](#)

[Board of Directors](#)

[Independent Living Community Services \(ILCS\)](#)

[Careers](#)

[Discrimination Complaints](#)

SERVICES

[Managed Long-Term Services & Supports \(MLTSS\)](#)

[Comprehensive Care Management \(CCM\)](#)

[Nutrition Support Services \(NSS\)](#)

[Third-Party Administration \(TPA\)](#)

[Management Services Organization \(MSO\)](#)

